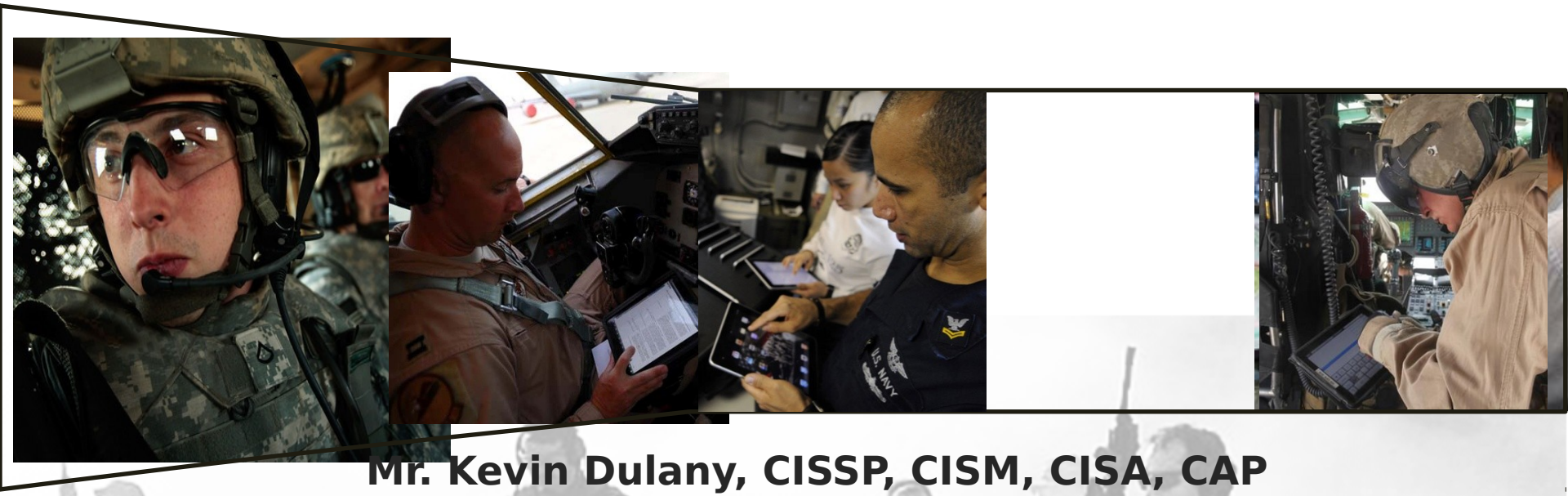
# Cybersecurity and the Risk Management Framework (RMF)

*Day 777 and Counting*

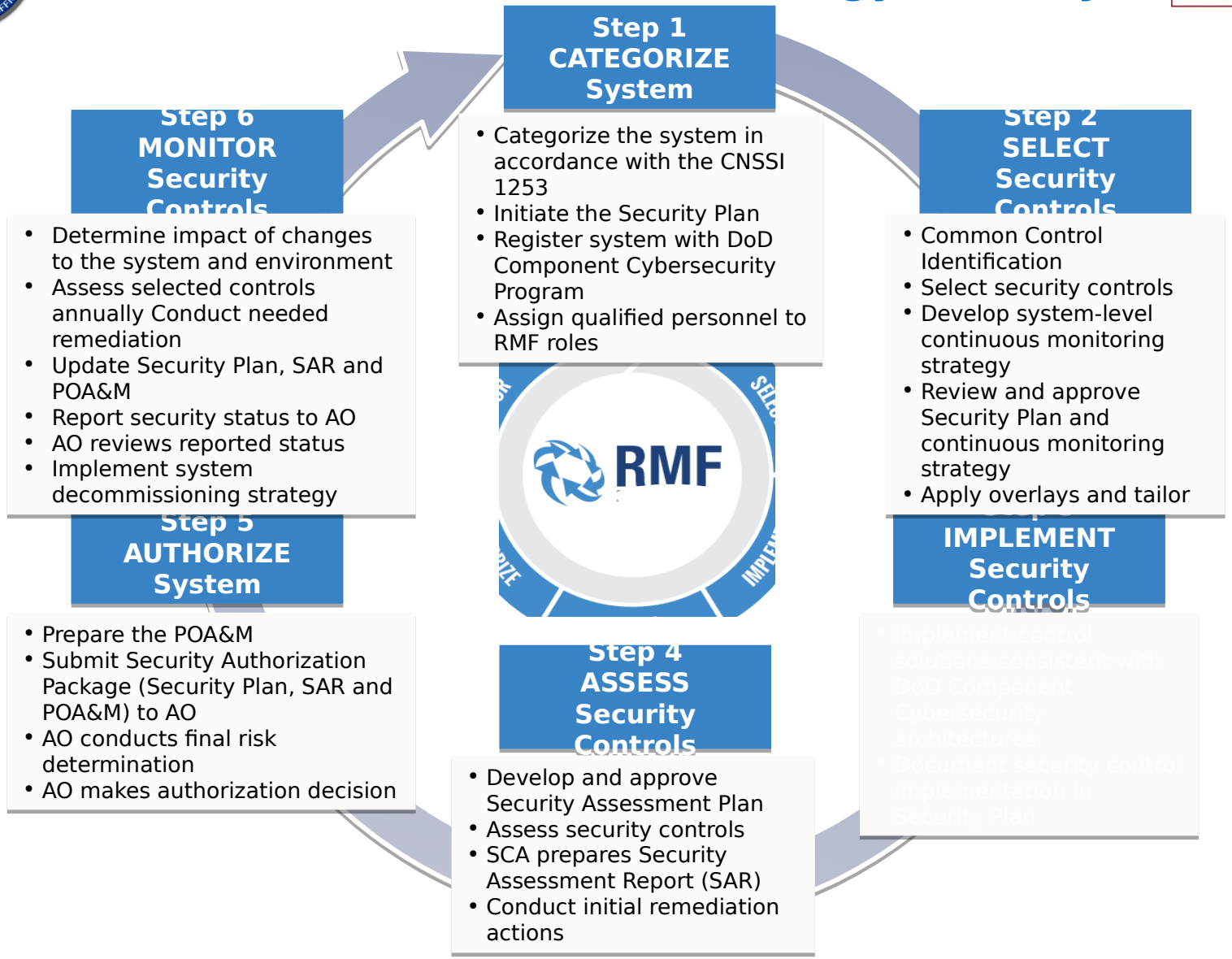


**Mr. Kevin Dulany, CISSP, CISM, CISA, CAP**
**Chair, RMF TAG, Department of Defense (DOD) Chief Information Officer (CIO)**
**Deputy CIO for Cybersecurity**
**Cybersecurity Policy & Strategy Directorate**

**Mr. Tim Denman**
**Cybersecurity Learning Director**
**Defense Acquisition University**

# Agenda

# RMF Process for DoD Information Systems and Platform Information Technology (PIT) Systems


Step 1
CATEGORIZE System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve Security Plan and continuous monitoring strategy
• Apply overlays and tailor
Step 3
IMPLEMENT Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in Security Plan
Step 4
ASSESS Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE System
• Prepare the POA&M
• Submit Security Authorization Package (Security Plan, SAR and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR Security Controls
• Determine impact of changes to the system and environment
• Assess selected controls annually Conduct needed remediation
• Update Security Plan, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy
RMF

# February 2016 DoD AO Summit Highlights

**Meeting Objective**

Briefing of RMF lessons learned by DoD CC/S/As

**AO Summit Briefers**

- AF
- Navy
- Army
- USTRANSCOM
- USPACOM
- USSTRATCOM
- DISA
- DTIC
- JIDA

# Cybersecurity Reciprocity Process

## Receiving Component Activities

### Monitor and Communicat

Per SLA/MOU/MOA communicate any changes to system or hosting environment that impacts security/mission

### Update

Update security packages based on any inheritance relationships or security changes

### Approve

- Enclave approves connection [*Enterprise systems: ISRMC Designates IS as Enterprise Approved]*
- Document in SLA/MOU/MOA

## Deploying DoD Component Activities

### Initiate

- Initiate negotiations with receiving enclave/sites
- Initiate the security authorization package

### Authorize and Communicat

- IS is authorized by Component AO
- Made visible to receiving enclave/ site *[Enterprise systems: DSAWG]*
- Address additional security requirements as identified

### Register

Register in VMS & PPSM Registry for enterprise-level vulnerability management

### Share

- **Deploying DoD Component** provides decision briefing with receiving enclave [*Enterprise systems: ISRMC]*
- **Receiving Component** ensures visibility of security authorization package

## Reciprocity

...Codifies tenets ensuring IT is developed and fielded consistently, rapidly, and efficiently across the enterprise

Recommendations to improve reciprocity process:

- Ensure the assessors meet an accepted standard (e.g. FedRAMP, 3rd Party Assessor) – provide evaluation requirements in workforce policies for individuals (SCAs) and team
- Develop a program for evaluating and accrediting security control assessors and their teams
- Understand that acceptance of documentation depends on mission and environment risk tolerance
- Acknowledge that AOs should not repeat a security assessment but reuse another organizations assessment to the greatest extent possible to inform risk decisions

# Other Miscellaneous RMF Issues

| Issues | Solutions |
|---|---|
| How to assess non-traditional IT | Establishment of guidance through the RMF KS (e.g., EI&E PIT Control Systems page) |
| Increased amount of security controls | Promoting leveraging of automation (e.g., eMASS, ISCM) |
| Continuous Monitoring risk scoring | CMRS will help identify if assets are configured securely, update configurations, and provide insights into how to optimally apply defensive resources. |
| AO Reduction | Continue to survey Components and working with the AO Summit members |
| RMF Training | Various training available from DISA and DAU |
| SCA Standardization | Coordinating with NIST to establish Federal-wide standards |
| DoD RMF Overlay Process | Guidance on the RMF KS that leverages |

# RMF – Keys to Success

1. Involve cybersecurity experts before Milestone A
2. Apply cybersecurity principles throughout the acquisition lifecycle
   - System design and architecture
   - Supply chain risk management
   - Software Assurance
   - Continuous monitoring
   - Test and Evaluation (T&E)
3. Promote cybersecurity knowledge and best practices across career fields
   - It all starts with the contract and requirements
   - It's about risk management, not risk elimination. PM must understand trade offs and set the tone
   - Use testing teams (blue, red, green, …) wisely and effectively
   - There is no substitute for government oversight (Engineers, Logisticians, T&E, IT, …)
   - Career field specific training is essential

# DoD Cybersecurity Workforce Training

- DoD Directive 8140.01 (Cyberspace Workforce Management – 08/11/15) replaced DoDD 8570.01
  - Establishes a DoD Cyberspace workforce management council
  - Unifies the cyberspace workforce and establishes workforce elements to manage cyberspace workforce roles
- NICE identifies critical knowledge, skills & abilities for job roles.
  - Emphasizes hands-on experience and training
  - Organizes the workforce into 7 Categories and 32 Specialty Areas

***NICE Framework (tailored for DoD specific issues) will serve as basis for DoD Instruction 8140.01, which will replace DoD 8570.01-M.***

# NICE National Cybersecurity Workforce Framework

- The National Cybersecurity Workforce Framework provides a blueprint to categorize, organize, and describe cybersecurity work into Specialty Areas, tasks, and knowledge, skills and abilities (KSAs).
- Consists of seven categories, 32 specialty areas grouped within the seven categories, and a list of associated knowledge / skills / abilities

| Category | Responsible For: | Specialty Areas |
|---|---|---|
| Securely Provision | Conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development | IA Compliance, Enterprise Architecture, Sys Req Planning, Sys Development, SW Engineering, Tech Demonstration, Test & Evaluation |

***Knowledge, Skills & Abilities (KSA) for each competency within the NICE framework will be a major driver for future DAU training.***

# NICE Core KSAs

| Item ID | KSA | Statement | Competency |
|---|---|---|---|
| 22 | KSA | Knowledge of computer networking concepts and protocols, and network security methodologies. | Infrastructure Design |
| 108 | KSA | Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). | Risk Management |
| 1157 | KSA | Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity. | Legal, Government, and Jurisprudence |
| 1158 | KSA | Knowledge of cybersecurity principles. | Information Systems/Network Security |
| 1159 | KSA | Knowledge of cyber threats and vulnerabilities. | Vulnerabilities Assessment |

# DAU RMF and Cybersecurity Training

- On-line
  - CLE 074
  - ISA 220 (RMF for Practitioners) to be deployed in FY 17
  - Courses in development on Program Protection Planning, Software Assurance, and Supply Chain Risk Management
  - Videos and website (AAP)
- Classroom
  - ISA 101, 201, 301 and 302 (new content)
  - Classes with updated cybersecurity content include ACQ 203, TST 204, and others (based on FIPT demand)
- Workshops
  - 2 to 5 days walking programs/organizations through the six steps of the RMF
  - Tailored to specific program or organization
  - Designed for 15 to 30 people and is on location with 2 to 3 instructors
  - Usually the only costs are travel expenses for instructors

# Additional Sources of RMF Training

- **DISA: AO RMF training course (3-4 hour CBT)**
  - Training required by DoD 8570.01-M. https://powhatan.iiie.disa.mil/eta/disa_ao_fy14/launchpage.htm.
- **DISA: RMF for DoD IT course (3 hour DCS)**
  - General RMF practitioners (high level intro course). http://iase.disa.mil/rmf/Pages/rmf-training.aspx
- **DSS: RMF training course (4-5 hour CBT)**
  - General RMF practitioners; http://www.cdse.edu/catalog/cybersecurity.html
- **NDU / iCollege: Focused on RMF in an educational context (in residence)**
  - Enterprise Information Security and Risk Management & Authorization to Operate (ATO) courses
- **NIST: Applying the RMF to Federal Information Systems (2 hour CBT)**
  - High Level RMF introduction; http://csrc.nist.gov/groups/SMA/fisma/rmf-training.html
- **eMASS Training**
  - Online CBT or instructor led training is also available; https://powhatan.iiie.disa.mil/emass/training.html

# Resources for Policy

| Title | Purpose | Link |
|---|---|---|
| **Knowledge Service** | DoDI 8510, Authoritative RMF Guidance | https://rmfks.osd.mil/ |
| **DISA IA Support Environment** | STIGs, CCIs, SRGs, DAA/AO Training | http://iase.disa.mil/index2.html |
| **DoD Issuances Website** | DoDI 8500.01, DoDI 8510.01 | http://www.dtic.mil/whs/directives/index.html |
| **CNSS Policies** | CNSSI 1253, Security Control Categorization and Selection | http://www.cnss.gov/policies.html |
| **NIST Publications** | NIST SP 800-53 Rev. 4 Security controls, NIST SP 800-37, Guide to implementing RMF | http://csrc.nist.gov/publications/PubsSPs.html |

**Mr. Kevin M. Dulany**
**Chief, Risk Management Framework Division**
DOD CIO, DCIO(CS), CSPS
Kevin.M.Dulany.civ@mail.mil

**Email RMF Implementation Questions to:**
RMF TAG Secretariat (OSD.RMFTAG-Secretariat@mail.mil) or via the RMF KS Help and Feedback Form (https://rmfks.osd.mil)

**Mr. Tim Denman**
**DAU Cybersecurity Learning Director**
Tim.Denman@dau.mil
or
Acquisition.CyberSecurity@dau.mil

# BACK-UP

## Current RMF Transition Period Requirements

Enclosure 8, DoDI 8510.01, "All IS and PIT systems must transition to the categorization and security controls selection methodology, security control catalog, and the RMF within 3 years and 6 months from the effective date of this instruction."

| System Authorization Status | Transition Timeline And Instructions |
|---|---|
| New start or unaccredited | Transition to the RMF within six months |
| System has initiated DIACAP but has not yet started executing the DIACAP Implementation Plan | Transition to the RMF within six months |
| System has begun executing the DIACAP Implementation Plan | **Either:**<br>a. Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline **or,**<br>b. Transition to the RMF within six months |
| System has a current valid DIACAP accreditation decision | Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline |
| System has a DIACAP accreditation that is more than 3 years old | Transition to the RMF within six months |

# Overlays

…Enterprise-wide overlays will create efficiencies through standardized tailoring

- Overlays address additional factors beyond the standard baselines
- Enterprise Tailoring - Consistent approach and set of security controls by subject area allowing for risk decisions to be made up

| Approved CNSS Overlays | Approved DoD RMF Overlays |
|---|---|
| • Intelligence (FOUO, revision in progress)<br>• Space Platform (revision to 800-53, Rev. 4 – TBD)<br>• Cross Domain Solutions (revision in progress)<br>• Classified Information (based on 800-53, Rev. 4)<br>• Privacy (including PHI) | • Nuclear, Command and Control, Communication Systems (USSTRATCOM) |

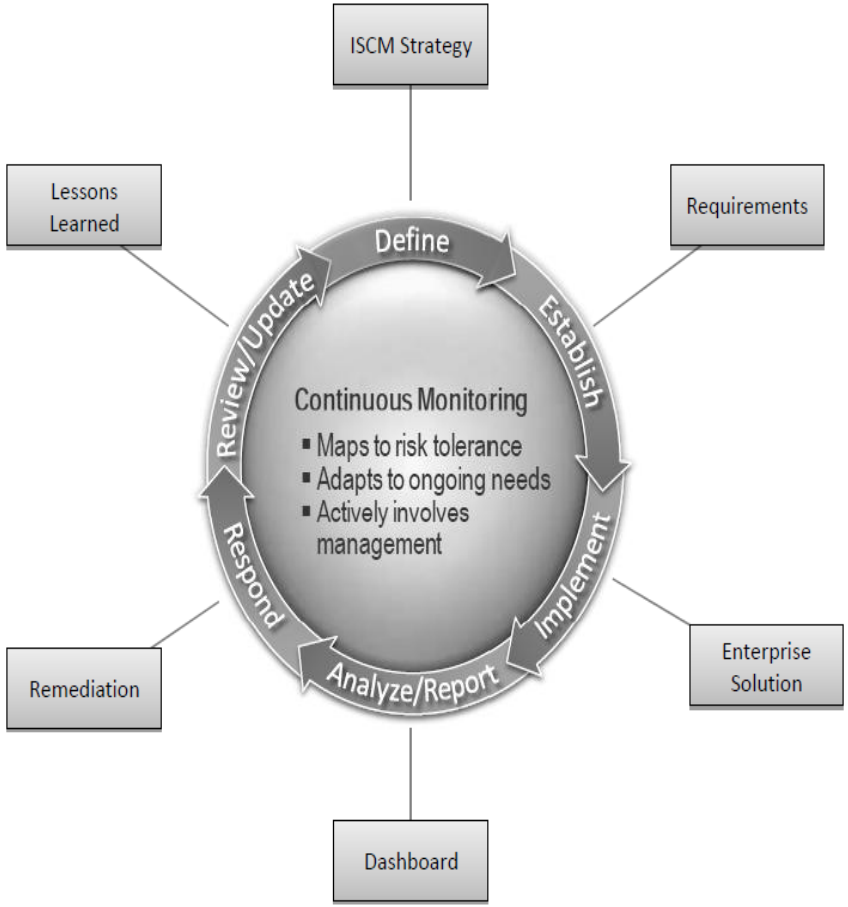
# DoD RMF Overlay

- DoD RMF Overlay Development Guidance *(Reviewed by the RMF TAG and will be made available on the RMF KS)*
  - Leverages CNSS guidance and the CNSS 1253F Attachment 1: Security Overlays Template
  - DoD RMF overlay development is overseen by the Functional Mission / Capability Owner and overlay proponent, with the RMF TAG serving in a primarily advisory role
  - DoD RMF overlays will be housed on the RMF KS (e.g., NC3 Overlay)
- DoD Enterprise RMF Overlay vs. DoD Component RMF Overlay:
  - DoD RMF overlay approval:
    - Enterprise: Functional Mission / Capability Owner
    - Component: Component Mission Owner
  - Location of DoD RMF overlays:
    - Enterprise: RMF KS Page “Overlay Application and Selection”
    - Component: RMF KS Component Workspace
  - Implementing the overlay within eMASS
    - Enterprise: All instantiations
    - Component: Individual instantiations based upon request

# Continuous Monitoring and Continual Reauthorization

…Emphasizes continuous monitoring and timely correction of deficiencies

- RMF is necessary to set the baseline for the initial authorization (i.e, meeting CS expectations)
- Developing the programmatics for institutionalizing ongoing authorization (supports 3 year reaccreditations) by leveraging a robust Continuous Monitoring Program, and developing joint processes to adopt reciprocity for cybersecurity across DoD the IC, and Federal Civilian Agencies
- 3 year reaccreditations will see significant reduction in time and cost



# Current State of ISCM

## TOP 3 PRIORITIES:

- Actionable security risk scoring
- Improve implementation of core CS tools
- Augment CCRI, FISMA reporting, enable Ongoing Authorization processes

## Value Proposition

- **Why it's important**: Actionable risk scoring reduces cybersecurity risk to DoD information networks. We must increase the efficiency of cybersecurity tools to deliver comprehensive monitoring of cyber key terrain, to detect intrusions, protect assets, and defend against exploitations.

- **What happens if we don't do it**: Without ISCM the Department will continue poor organizational response to threats and vulnerabilities, uneven execution of manual security processes, and redundant Service/Agency investments in cybersecurity technologies that lack interoperability.

## Description

- ISCM is a framework of cybersecurity tools, processes, and technologies enabling security risk scoring

- Phase 1:
  - Host Based Security System
  - Cyber Operational Attribution Management System
  - Digital Policy Management System
  - Continuous Monitoring/Risk Scoring Systems (CM/RS)

- Current Efforts: asset tagging standards, actionable risk scoring
- Current Gaps: automated patch and vulnerability management. Strategic Initiatives: reduce FISMA reporting costs; inform CCRI efforts; enable On-going Authorization; automate DoD Connection Approval Process.

## Deliverables: FY14-FY16

- ✓ ISCM Strategy
- ✓ JS Validation of ISCM and C2C Operational Requirements
- ✓ ISCM Cybersecurity Tool/Capability Analysis
- ✓ DoD Operational Attributes and Asset Tagging Standards
- ✓ ISCM Implementation Plan
- ✓ ISCM Data Strategy
- ✓ Joint Issue Paper for DoD Comply to Connect (C2C)
- ✓ Analysis of current host based security Implementation
- ✓ = efforts in progress/near completion
- ◆ = efforts not started

# ISCM Strategy

## ISCM VISION

Enhancing mission assurance through actionable cybersecurity risk scoring

## MISSION

To maintain continued visibility into the cybersecurity state of DoD information resources

**OUTCOME:** To operate in a trustworthy Defense Information Environment free from known cybersecurity vulnerability

## GOALS AND OBJECTIVES

Objective 1: Create the operating environment to support actionable security risk scoring
Objective 2: Create an operationally relevant risk score
Goal 2: Configure information systems right - keep them right
Objective 1: Reduce opportunities for cybersecurity exploitation
Objective 2: Drive configuration compliance
Goal 3: Create opportunities for process efficiencies
Objective 1: Augment security assessments, federal compliance reporting, cybersecurity risk adjudications
Objective 2: Automate to drive process standardization
Goal 4: Drive cultural change
Objective 1: Use actionable risk scoring to remediate operationally vulnerable assets
Objective 2: Transition from cybersecurity compliance to cybersecurity readiness

## FY14 – FY16 PHASE 1 PERFORMANCE METRICS

**CHARACTERIZING THE ATTACK SURFACE**

- % of Components registered and using ISCM
- #s of assets monitored for risk scoring
- % of Icyber key terrain identified for monitoring

**REDUCING THE ATTACK SURFACE BY DRIVING DOWN VULNERABILITIES**

- % of DoD Components actively remediating identified cybersecurity vulnerabilities
- #s of CS process results integrated into CM/RS for security risk scoring
- #s of Authorizing Officials using CM/RS results to augment their authorization decisions
- Average cost reduction identified as result of using ISCM for On-Going

## FY 17 – FY18 PHASE II PERFORMANCE METRICS

**SENSING AND RECOGNIZING ADVERSARIAL BEHAVIOR**

- % of DoD Components implementing a host intrustion/detection capability
- #s of cyber warnings and indicators to erradicate false indicators of threat

**MANAGING INFORMATION AND THE TRUSTWORTHINESS**

- % of near real-time vulernabilities detected and reported using ISCM
- % of Deployed capabilities actively detect ing and report ing unauthorized requests for DoD information

# DoDI 8500.01 "Cybersecurity"

- Expands and clarifies applicability of cybersecurity to all IT that receives, processes, stores, displays, or transmits DoD information, including computing embedded in weapons systems and industrial control systems
- Covers all DoD information regardless of where the information may reside, puts emphasis on driving anonymity out of the networks, and applies to every DoD organization
- Enables deployment of enterprise-wide cybersecurity solutions (i.e. build once, use by many) via inheritance of centrally built, hosted, and authorized capabilities, giving commanders more freedom of action in DoD networks
- Aligns DoD with rest of federal government by adopting National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) standards, promoting interoperability and information sharing.
- Vendors may now build products once according to NIST guidelines and then more readily deploy them government-wide saving time and money and fostering reciprocity
- Ensures mission risk and mission resilience are central to program

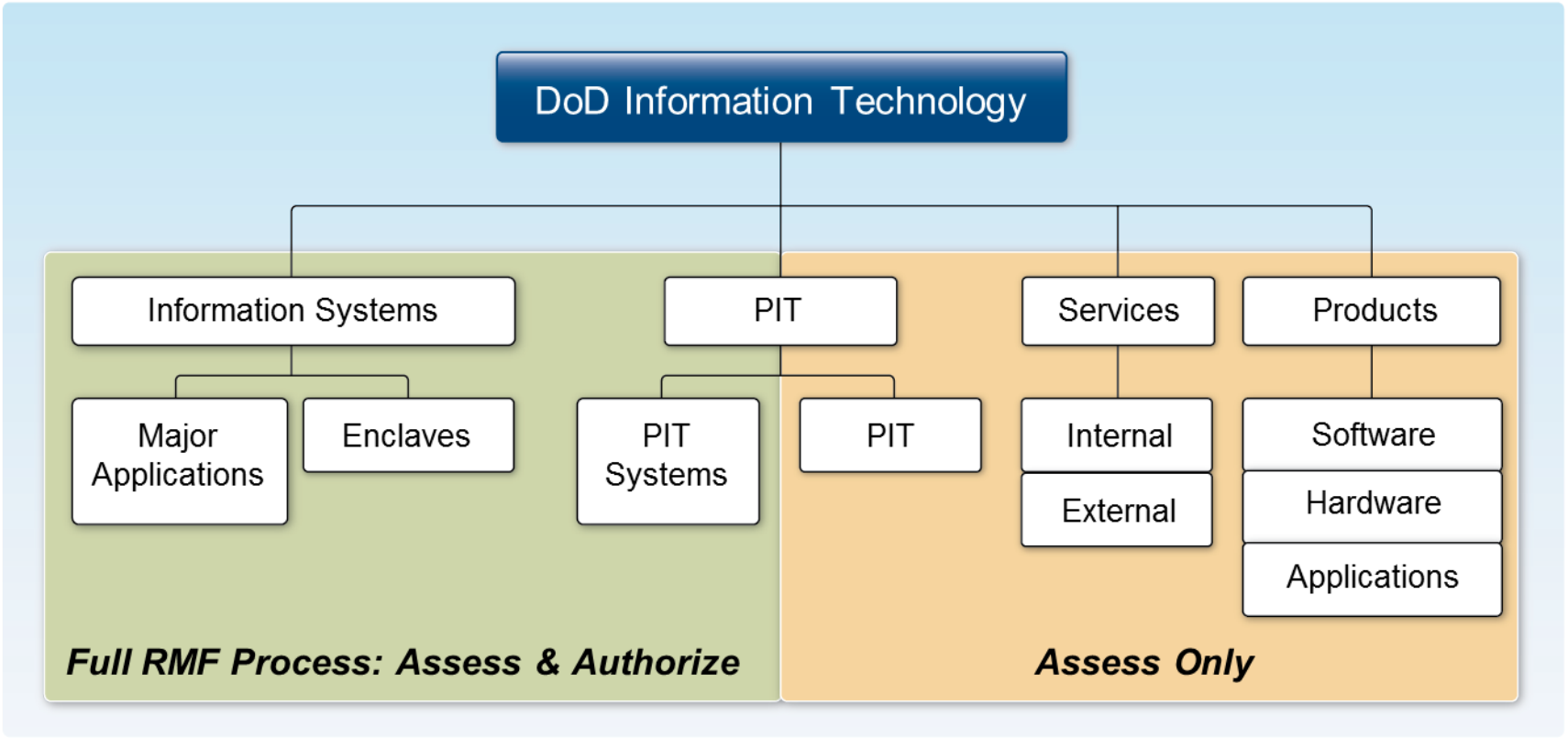
# DoDI 8510.01 “RMF for DoD IT”

- Incorporates cybersecurity early and robustly in the acquisition and system development lifecycle
- Implements a three-tiered approach to risk management that addresses risk-related concerns at the enterprise level, the mission and business process level, and the information system level
- Focuses on risk to the mission and buying down cybersecurity risks through the right mitigations
- Provides a risk management methodology that gives organizations a true picture of vulnerabilities caused by non-compliant controls as it relates to other risk factors (i.e. likelihood, threat, and impact)
- Codifies system authorization reciprocity, enabling organizations to accept approvals by other organizations for interconnection or reuse of IT without retesting
- Emphasizes information security continuous monitoring and timely correction of deficiencies, including active management of vulnerability and incidents
- Applies to all IT which reduces exploitation of vulnerabilities in PIT,

# RMF applies to all Information Technology

…Reduces exploitation of vulnerabilities in PIT, Services, or Products previously not secured or assessed

*"All DoD-owned or DoD-controlled IT that receive, process, display or transmit DoD information"*




*Not a one size fits all approach to securing IT*

# DoD leverages and builds upon numerous existing Federal policies and standards

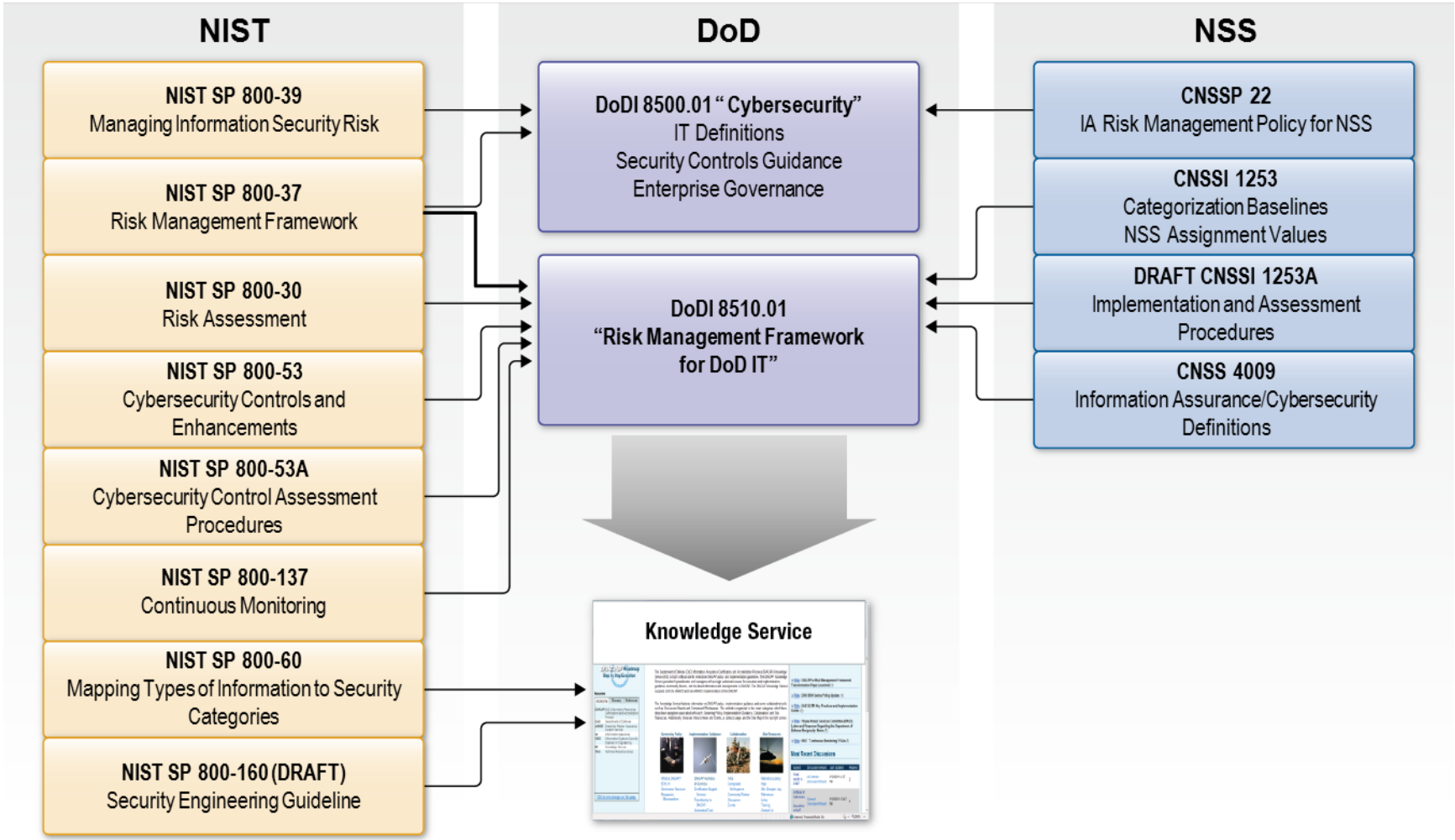
…Less DoD policy to write and maintain

*DoD participates in development of CNSS and NIST documents ensuring DoD equities are met*

*DoD leverages CNSS and NIST policies and filters requirements to meet DoD needs*

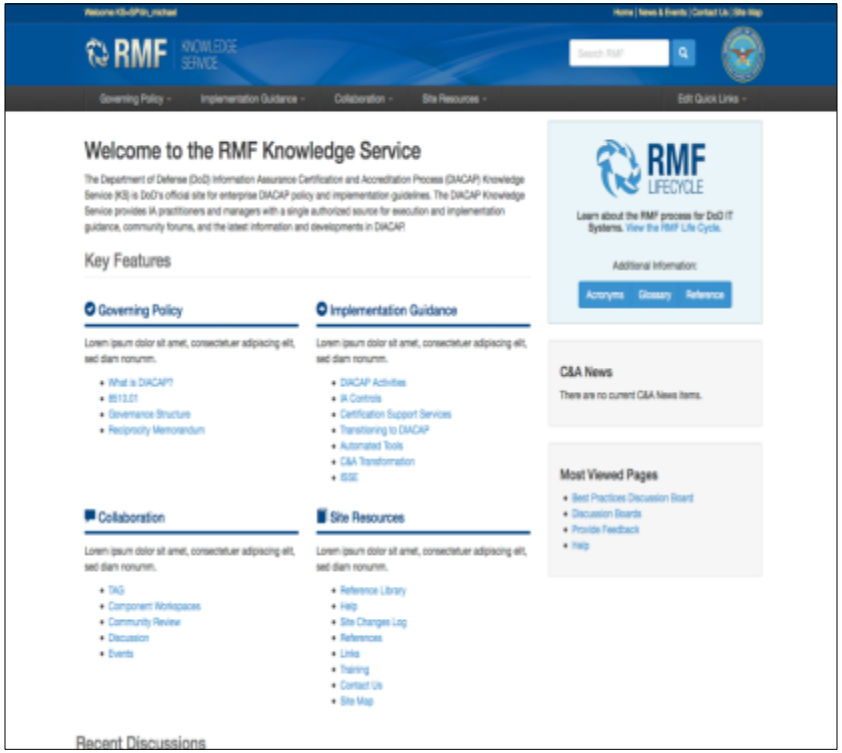
*DoD participates in CNSS and NIST policy development as a vested stakeholder with the goals of a more synchronized cybersecurity landscape and to protect the unique requirements of DoD Missions and warfighters*

# Cybersecurity Policy Alignment



# DIACAP / RMF Knowledge Service

...The authoritative source for information, guidance, procedures, and templates on how to execute the DIACAP and Risk Management Framework




**https://rmfks.osd.mil**

# RMF Technical Advisory Group (RMF TAG)

- **Mission**: Strengthen and evolve the ability for DoD to rapidly deploy secure IT systems that enable information sharing between the Department, the IC, and other entities.
- **Duties**:
  - Provide implementation guidance for the RMF
  - Provide detailed analysis and authoring support for the enterprise portion of the Knowledge Service (KS)
  - Recommend changes to security controls, baselines, and RMF policy
  - Advise DoD forums established to resolve RMF priorities and cross-cutting issues
  - Develop and manage RMF automation requirements
- **Chair**: DoD SISO appointed
- **Members**: All DoD Components are authorized to be represented by one primary and one alternate cybersecurity SME.

***Email questions regarding the RMF TAG and its efforts to: RMF TAG Secretariat (OSD.RMFTAG-Secretariat@mail.mil)***

# eMASS Overview

- **Enterprise-level web-based system** establishing a standard approach to DIACAP and RMF processes to develop, collect, manage, and generate cyber-security related data and reports across DoD organizations.
- **DISA-Sponsored Enterprise Service** and GOTS solution centrally managed by DISA ID5 currently deployed on NIPR and SIPR. Minor releases every two months and major releases every 6 months.
- **Role-based management** of users with customizable organizational taxonomy, workflow, and access to enable workload management and enforce accountability.
- **Maintenance of an enterprise baseline for security controls** in accordance with the NIST SP 800-53 and CNSSI 1253.
- **DoD cyber solution compatibility** allows eMASS to consume outputs from vendor/COTS/GOTS scanning tools and map results to information systems including ACAS and HBSS Policy Auditor. Integration with VMS.
- **Enterprise-level visibility** of all authorization packages offering comprehensive organizational security posture dashboard reports including Top Non-Compliant Controls and DIACAP to RMF Transition tracking

***Email questions regarding eMASS to: eMASS Help Desk Support (*** disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mi)

# Revised RMF Transition Timeline & Instructions

| Completed DIACAP Package Submitted to Authorizing Official for Signature | ATO Date | Maximum Duration of ATO under DIACAP |
|---|---|---|
| September 17, 2015 through May 31, 2015 | Determined by AO Signature Date | 2.5 years from AO signature date |
| June 1, 2015 through February 1, 2016 | | 2 years from AO signature date |
| February 2, 2016 through October 1, 2016 | | 1.5 years from AO signature date |

# Revised RMF Transition Period

- Change 1 to DoDI 8510.01 in formal coordination
- Establishes a new RMF initial transition timeline
  - Supersedes *RMF Initial Transition Timeline and Instructions,* Table 2 within Enclosure 8, DoDI 8510.01
  - Allows flexibility to manage the transition schedule preventing a surge of DIACAP ATOs
- Addresses comments on technology and training supporting the RMF
  - Provides DoD SISO responses to commonly requested DIACAP to RMF information
  - Covers the following areas: overlays, eMASS, training, RMF Knowledge Service, common controls (DECC specific), CNSSI 1253 transition

# Cybersecurity Discipline

**We need to develop and reinforce a healthy cybersecurity culture.**

## Overview

**DoD CIO and USCYBERCOM chartered a Tiger Team with representatives from Services and Agencies to identify immediate actions to strengthen basic cybersecurity readiness**

**Commander engagement**

- Ensure unit leadership involvement in cybersecurity via readiness reporting

**Enforce current policy**

- Focus on most important tasks in the Cybersecurity Scorecard and existing policy

## Lines of Effort

**1. Enforcing Strong Authentication:**

Eliminate use of username/password logon in favor of two-factor DoD PKI authentication for both privileged and non-privileged users

**2. Device Hardening:**

Improve patching practices, reduce e-mail as a vector, and increase the HBSS footprint across DoD information networks

**3. Reduce the Attack Surface:**

Contain internet connections to the DODIN to approved DMZs; eliminate back doors and lateral movement within the DODIN core

**4. 100% CNDSP Alignment:**

Align all units/components with an

# DoD Cybersecurity Scorecard Overview

- **DoD Statistics**:
  - Thousands of DoD Networks
  - 7 million connected devices
  - 250,000 intrusion attempts on DoD networks every hour
- **Virtually all successful cyber attacks against DoD and others exploit preventable vulnerabilities**
- **Attacks against these are cheap, fast to develop, fast to modify**
  - Cyber defenders struggle to keep up. Real operational vulnerability for DoD
- **Efforts to prevent this vulnerability are called *cybersecurity discipline***
  - Already mandated in policy, technical direction, orders
  - Yet many exploitable, preventable vulnerabilities persist in DoD

# DoD Cybersecurity Scorecard Overview cont

**CIO, Cyber Command, led team of experts from throughout DoD to address urgent cybersecurity discipline issues.**

- **Tiger Team Concluded:**
  1. ***Accountability* via chain of command is key**
     - Measurement and reporting of progress and steady state are essential
       - Some items via readiness system
     - Current measurement insufficient, improved automation needed
  2. ***Prioritization* of effort is key**

- **Produced prioritized mitigation list, with plans**

- **Documented in *Cybersecurity Discipline Implementation Plan***
  - *Mr. Halvorsen, ADM Rogers and Mr. Kendall signed the Cybersecurity Campaign memo on 12 June 15.*

# Key Takeaways

- **Cybersecurity is a Senior Leadership Priority**
  - SECDEF / DEPSECDEF monitoring monthly
  - CIO-level weekly drumbeat meeting for “getting green”
    - Prudently

- **Cybersecurity culture change required at all levels**

- **Cyber Scorecard is an evolving, living document.**
  - New metrics will be added over time
  - Coverage outside NIPRNet & SIPRNet